Copy to H.C.S.G.
25/9.

15(Q)

TOP SECRET - 1 - TICOM/I-103

SECOND INTERROGATION OF REG. RAT HERMANN SCHERSCHMIDT OF PERS. Z S AUSWÄRTIGES AMT, ON TURKISH AND BULGARIAN SYSTEMS.

(11)

Attached is a report on an interrogation carried out by Major BUNDY at the U.S. 7th Army Interrogation Centre, on 29 August 1945, covering Turkish and Bulgarian Systems solved by Pers. Z S.

See Ticom/I-63 for previous report.

TICOM

19 Sept. 1945 No. of pages 4

DISTRIBUTION

British

D.D.3
H.C.G.
D.D. (N.S.)
D.D. (M.W.)
D.D. (A.S.)
C.C.R. (2)
Lt. Col. Leathem
Cdr. Tandy
Major Morgan

U.S.

Op-20-G (2) (via Lt. Cdr. Manson)
G-2 (via Lt. Col. Hilles)
A.S.A. (3) (via Major Seaman)
Director, S.I.D. USFET
(via Lt. Col. Johnson)
Col. Lewis Posell, USSTAF

TICOM

Chairman
S.A.C. (2)
Cdr. Bacon
Lt. Col. Johnson
Major Seaman
Lt. Cdr. Manson
Capt. Cowan
Lt. Fehl
Ticom Files (4)

Additional.

Lt. Col. Thompson.

Introductory:

It had been requested that SCHERSCHMIDT should do a complete written paper on his work on Turkish and Bulgarian systems. As his eyes, after a recent operation, do not yet permit reading, the subjects were covered by interrogation instead. His memory is sketchy on many points, but it seems unlikely that a written account based on further recollection would add much substance to this account.

1. Turkish systems

a) Diplomatic.

The Auswärtiges Amt did not work on Turkish at all until 1934. S. believes that there was in fact very little Turkish traffic until after the MONTREUX Conference in that year. He had worked on Turkish in 1920 and believes that the codes remained basically the same (alphabetic, with Arabic lettering) until 1934.

1934 - early 1935. The main system in this period was a set of 3 4-digit codes used in monthly rotation. The codes were alphabetic within any one initial letter, but the order of the letters was scrambled. The codes were rarely used without encipherment by a

section, while SCHERSCHMIDT himself concentrated on book-building and translation, occasionally checking the work of the girls in case of difficulty. Book-building and translation were fairly difficult, because of the use of the Arabic lettering and because SCHERSCHMIDT himself was only learning Turkish as he went along.

The auxiliary system, used for less important traffic, had a single code, completely unalphabetic. Though theoretically more difficult, the code was used about half the time without encipherment and was built up accordingly, aided by one or two isolated cases of reencodement from the main system. The encipherment system, when used, was the same as for the main system and was solved in the same manner.

The two systems covered all the main diplomatic links. S. believed that there were other codes used for isolated links, as RIO DE JANEIRO and BUENOS AIRES, but there had never been enough material for a solution of these.

1935 - 1939. In 1935 the Turks switched abruptly to the latin system of literation and issued a new main system consisting of 3 codes used in monthly rotation as before. The old set of three Arabic-lettered codes was made fully alphabetic and was used as an auxiliary system for consular traffic.

the same solution technique was used as before. The code was at

The basic set of latin codes remained in use until 1939, when S. left the section. The codes were scrambled by sections in 1938; but the thread was quickly regained.

1939 - 1944 S.'s knowledge of the period is vague as he handed the section over to BENZING in 1939. When he wished to return to Turkish in 1943 there was difficulty (though not with BENZING himself) over his status, and he left Pers Z S entirely for a year. S. finally resumed Turkish in 1944, being almost entirely occupied in translation in the last months of the war.

He believes the basic codes became entirely alphabetic in 1939. They were always enciphered, but he does not know the exact system, nor the exact details of solution methods. It is assumed that the basic technique remained the same, and that the stripping was done by the less skilled personnel, while BENZING and one or two others did the harder jobs of book-building and translation. Almost complete success continued.

In addition to the main system S. recalls an unalphabetic Latin-literation code used from SWITZERLAND; this he believes to be an older code which had been compromised. Still another code was used from AFGHANISTAN and beginning in 1944 from GREECE. At first this was not enciphered and the book was built up to enable solution of later enciphered AFGHANISTAN traffic.

2. Turkish systems

b) Military.

While the Auswärtiges Amt did not handle military traffic habitually, the Turkish military traffic was made available to them, and they tackled it when time permitted.

The first solutions were achieved in 1936-7 and continued until 1939, although there was very little traffic in this period. The code was 5 Z, and was sometimes enciphered by a primitive method taking only one or two digits of each group and leaving the rest unchanged. Solution was aided by a common "General Staff" address which came to four groups in the new Latin literation, and by one case of a direct reencodement from a message sent in the diplomatic code.

After 1939 a new code was introduced, and S. is unable to give any details of BENZING's work on it. He has the impression that spasmodic success was achieved, but the bulk of the work on this was done by OKW. (The OKW section was headed by REG. RAT Dr. LOCKER, and had more people than PERS. Z S. S. had a low opinion of the linguistic ability of the OKW translators, and did not think the results were in proportion to the numerical difference. He believes OKW had considerable success with Turkish military systems.)

3. Bulgarian Systems. S. stressed that this was not his main job and was done largely on a spare-time basis. Before 1938 Bulgarian work was not considered important at all, and only a few

scattered efforts were made. S. went to work on it in earnest only in the Summer of 1941.

The main system consisted of two basic codes, used on the same links for material of different security importance. The codes were 5 Z, with about 20- 30,000 actual values before 1939, and 30- 40,000 thereafter. The basic code was changed once between 1939 and 1944, S. thinks in 1941, and the former top security code then became the auxiliary system.

Except for one 2-3 month period the codes were not enciphered. Up to 20 links were served by providing a different pagination for the code twice a month on a single link. Within the pages the values were written in a cyclic alphabetical order, but the cycle might start in the middle of a page and run backwards or down and then up, or in a variety of ways.

Solution depended entirely on the amount of traffic. Any major link could be solved at will if the effort could be made, and in fact from 1943 on all major links were read. The basic code had been completely recovered by that time and the pagination could be built up correctly, with the aid of "Reference", numbers, special names, and lettered values which gave very common groups. The chief difficulty was to break the additional special pages provided for the use of each link, with personal and geographical names. As a whole solution was never a difficult technical operation.

S. knows nothing of Bulgarian military systems.